

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 17-CR-124-JPS

v.

MARCUS HUTCHINS,

Defendant.

**DEFENDANT MARCUS HUTCHINS' REPLY
IN SUPPORT OF OBJECTIONS
TO THE MAGISTRATE JUDGE'S ORDER AND
RECOMMENDATIONS**

The government's opposition to defendant Marcus Hutchins' objections to the magistrate judge's order and recommendations fails to consider fully and fairly the factual record; it ignores and misinterprets relevant caselaw; and it does not address and sometimes mischaracterizes certain defense positions. The Court should rule in Mr. Hutchins' favor and grant his motion to suppress and motions to dismiss.

THE MOTION TO SUPPRESS

The government's opposition to the motion to suppress presents a skewed and flawed overview of Mr. Hutchins' arrest and interrogation. It also fails to

consider critical facts and caselaw that undermine its arguments, and it mischaracterizes the evidence and defense positions.

Despite the government's claims to the contrary, Mr. Hutchins has consistently maintained that his post-arrest interrogation was coerced and involuntary.¹ (*See Gov't Response ("Opp.") at 5 (Dkt. No. 114).*) A thorough and fair review of the evidence and law supports this position and therefore suppression. After the Court reviews the filings, hearing transcript and exhibits (including listening to the partial audio recording of Mr. Hutchins' post-arrest interrogation), the defense submits this is the only decision the record supports.

A. The Government's Incomplete Factual Narrative

At the outset, the government offers an incomplete narrative of what transpired on the day of Mr. Hutchins' arrest and his subsequent calls from jail. (*See Opp. at 5-8*). The government's overview notably does not mention important evidence that came out at that hearing, all of which is discussed in the Mr. Hutchins' objections to the magistrate judge's order and recommendations ("Objections"), such as:

- The FBI agents' coordination of their testimony.

¹ This position was articulated in the original motion seeking suppression, in all subsequent defense briefing, and at the evidentiary hearing itself. (*See, e.g., Dkt. No. 55 at 2.*) The magistrate judge also did not note a "shifting" defense theory (because there was none), despite denying the motion to suppress.

- Mr. Hutchins' arrest was designed to confuse him about its true nature.
- The agents' failure to inquire about his drug use over the course of the days and hours before they questioned him.
- The agents did not show Mr. Hutchins the arrest warrant until near the end of his interrogation, nor did they even bother to describe the charges against him and where they emanated from.
- The partial audio recording of the interrogation, which does not reflect any alleged advisement to Mr. Hutchins of his rights or his signing of the Advice of Rights form.
- Agent Butcher's admission that she altered the Advice of Rights form.

(Obj. at 6-12.) And to the extent the government discusses the purported evidence adduced at the hearing, it offers an uncritical presentation of the agents' claims of what happened, failing to mention material countervailing facts.

For example, the government claims Agent Chartier told Mr. Hutchins he was under arrest pursuant to a federal arrest warrant, doing so in the stairwell after leading him out of the airport lounge. But by his own admission, Agent Chartier did not explain the nature of the charges or where they had been brought. (Tr. 19:25-20:4; 58:25-59:1.)

Agent Chartier also did not, in fact, mention a federal arrest warrant to Mr. Hutchins in the stairwell. His evidentiary testimony that he did is inconsistent with what he told the prosecuting attorneys when they prepared him to testify,

namely, only that he told Mr. Hutchins he was under arrest, not that it was a federal case or there was an arrest warrant.²

The government alludes to this problem when it discusses how the defense sought to call one of the prosecuting attorneys to testify at the evidentiary hearing. (*See Opp.* at 5 n.2.) The defense only made that request (and did not do it lightly) because the prosecutors were the only witnesses to Agent Chartier's inconsistent testimony on this point (as well as another piece of inconsistent testimony from Agent Butcher). (Tr. 155-56.) The Court should overturn the magistrate judge's ruling denying the defense's request, and at a minimum find Agent Chartier's evidentiary hearing testimony on this point not credible.

The government also claims that Mr. Hutchins, in a call placed from jail soon after his arrest, "stated he told the FBI that he wrote the code for a banking Trojan and that he sent a compiled malware binary to someone." (*Opp.* at 8.) Although the defense maintains its position the jail calls should not be considered,³ Mr. Hutchins actually said he "wrote code for a guy a while back who then incorporated it into banking malware. . . that person went in [sic]

² At issue is an e-mail—one that was referenced during the evidentiary hearing but not entered into evidence—sent by an AUSA to defense counsel and summarizing statements made by Chartier to the AUSAs. According to the AUSA's e-mail, Chartier advised that: "Once Mr. Hutchins and [he] were behind closed doors leading to a stairwell, Mr. Hutchins was placed in handcuffs and told that he was under arrest. Mr. Hutchins asked why he was arrested, and he was told that once in an interview room they could talk further."

³ See Dkt. No. 75 at 12.

turned and took the code and used it to do banking malware.” (Ex. 2 at 7.) At most, Mr. Hutchins said he wrote a piece of code that someone else used to create a banking Trojan. The government can point to no statement from jail by Mr. Hutchins that he knew what would be done with the code he wrote.

Finally, the government fails to note that the alleged activities they questioned him about were historic, having taken place starting when Mr. Hutchins was only 18-19 years old (he was only 23 years old when interrogated), and Mr. Hutchins said during a jail call that he thought he may have been even younger at the time of some of the matters he was questioned about. (*Id.* at 8.)

B. The Government’s Reliance on the Magistrate Judge’s Findings Should be Rejected

After providing a partial overview of events, the government next spends considerable time reviewing the magistrate judge’s findings. (*See Opp.* at 8-10.) The government, however, concedes that this motion is subject to *de novo* review. (*Id.* at 4.) Thus, those findings are not entitled to any deference, and for the reasons explained in the Objections, they should not be accorded any.

C. The Government’s Overview of the Law Ignores Important Legal Precedent

The government offers an overview of what it considers the relevant law. (*See Opp.* at 10-12.) But the government, like the magistrate judge, ignores the Supreme Court’s important mandate, discussed on page 13 of the Objections,

that a court must “indulge in every reasonable presumption against waiver.”

Brewer v. Williams, 430 U.S. 387, 404 (1977).

The government instead spends time arguing that, because Mr. Hutchins understood English and had the Advice of Rights form presented to him before speaking, *Miranda* is satisfied. (Opp. at 11, citing *United States v. Springer*, 460 F.2d 1344, 1348-49 (7th Cir. 1972).) But this argument overlooks that deception and a defendant’s lack of full awareness can override this, as it does in the case of Mr. Hutchins’ interrogation. *See Moran v. Burbine*, 475 U.S. 412, 421 (1986).

D. The Government’s Arguments Regarding *Miranda* Waiver Confuse the Issues

The government’s discussion of Mr. Hutchins’ alleged waiver of his *Miranda* rights confuses the issues. The government contends that the defense for the first time in the Objections claims Mr. Hutchins was not advised of his rights. (See Opp. at 12, citing to Obj. at 17.) This is wrong and misleading.

In its post-hearing memorandum, for example, the defense noted that the timing of events, based on the FBI’s own records, does not support the agents’ version of events regarding when the advisement of rights occurred. (Dkt. No. 85 at 9.) The waiver form bearing Mr. Hutchins’ signature speaks for itself on the issue of whether he signed it. But the broader record raises serious questions and doubts about whether this Court can find that the advisement was properly given (e.g., the agents took the necessary time to give it and the time they claimed

they took) and that it occurred before interrogation. Upon those serious questions and doubts, and indulging every reasonable presumption against waiver as the law requires, the Court should find in Mr. Hutchins' favor.

This defense position is also not contrary to the record, as the government contends. (*See* Opp. at 12.) To support that argument, the government tries a neat trick: it cites for support a sentence in a brief the defense filed seeking an evidentiary hearing. (*Id.* citing Dkt. No. 55 at 10.) But that was before all the evidence on this matter had come out, including Agent Butcher's material alterations of the Advice of Rights form (which the defense at that time accepted at face value) and was not meant to be, nor was it, a concession. The defense has always challenged the government's version of events, and it still does. And taking seriously the presumption the law accords a defendant in a suppression context, the Court should too.

Importantly, the government, like the magistrate judge, ignores the numerous statements Mr. Hutchins made during his interrogation about how he did not understand what was going on, and Agent Chartier's admission that he had been misleading Mr. Hutchins into thinking the questioning was prompted by WannaCry. (*See, e.g.*, Ex. 1 at 00:30-00:32; 1:17:45-1:18:02.) Those statements are presented in detail on pages 19-24 of the Objections.

The government concludes this section of its argument by attempting to minimize the significance of Agent Butcher altering the Advice of Rights form well after the date of Mr. Hutchins' post-arrest interrogation. It is fair to infer that Agent Butcher altered the times written down because the timing was significant. The government does not address this fact. And as discussed in the Objections, the government should not be able to rely on a piece of evidence that a government agent intentionally altered in a material manner. (*See Obj.* at 24.)

E. There is Actually Evidence that Mr. Hutchins Was Impaired and Deceived, Despite the Government's Arguments to the Contrary

The government devotes seven pages to contending that there is no evidence that Mr. Hutchins was impaired or deceived during his interrogation. But in doing so it only selectively addresses defense points raised in the Objections and mischaracterizes the record and defense positions.

On the issue of impairment, the government calls the defense claims "pure, unsupported speculation that run counter [*sic.*] the record." (*See Opp.* at 14.) Untrue.

First, the defense discussed the significant holes in the evidentiary record on pages 15-16 of the Objections. For example, the government tries to minimize the agents' failure to inquire if Mr. Hutchins was on drugs, without acknowledging that the agents only arrested him when they did because they thought he might have ordered an alcoholic beverage. (*See id;* Tr. 65-67

(Chartier).) As another example, the government tries to make much of the fact that on the FBI's partial audiotape it appears that Mr. Hutchins unlocked his cell phones during the interrogation and claimed to be able do so when drunk. But plenty of people can do things when they are high they cannot do when they are drunk, and vice versa. (*See Opp.* at 15.)

Second, during the parts of the interrogation that the FBI recorded, Mr. Hutchins discussed partying, substance abuse, and a serious lack of sleep the night before his arrest and interrogation with the FBI agents. (Ex. 1 at 17:26-18:13; 58:53-59:09.) He described his time in Las Vegas as, essentially, a week-long party. (*See id.*) This is not mere defense speculation.

Turning to the agents' intentional deception, the record is full of examples of it. Rather than focus on that, the government begins its discussion of the topic by mischaracterizing the defense position. The defense has not argued that Mr. Hutchins "waived his rights under *Miranda* and confessed only because the interviewing agents refused to tell him that the investigation related to Kronos malware," as the government claims. (*See Opp.* at 16 citing to Tr. 206 (Closing Argument.)) The issue is not only that the agents not tell Mr. Hutchins that they had an arrest warrant out of this District related to Kronos – they completely hid the ball from him about why he was being questioned. And the Objections offer numerous examples of the agents' deception on pages 16-23, including those

drawn from the FBI's incomplete audio recording of the interrogation in which Mr. Hutchins' first question was simply "Can you please tell me what this about?"; a question Agent Butcher refused to answer. (Ex. 1 at 00:30-00:32.)

The government also tries to claim Mr. Hutchins would have spoken to the agents regardless, when it is clear from his repeated questioning that he would not have done so if he had known. (*See Opp.* at 17-18.) This argument should also not be entertained because it utterly undermines the clear intent of the case law dealing with deception (*i.e.*, if law enforcement has deceived someone, that person has not been given fair chance to weigh and waive his or her rights). *See United States v. Serlin*, 707 F.2d 953, 956 (7th Cir. 1983); *United States v. Giddins*, 858 F.3d 870, 885 (4th Cir. 2017).

The remainder of the government's arguments boil down to this: Mr. Hutchins must have known there was a criminal investigation, a circumstance overriding all of the agents' actions that confused and misled him. (*See Opp.* at 17-19.) Addressing the defense's citations to the numerous times the agents deceived Mr. Hutchins about the nature of his circumstance, the government argues:

But none of these examples show that the agents affirmatively misled [Mr.] Hutchins about the nature of their criminal investigation. Nothing the agents said dissuaded [Mr.] Hutchins from believing it was a criminal investigation.

(*Id.* at 19 (emphasis added) (internal citations omitted).) But this shows the government has missed the point. Whether Mr. Hutchins knew there was a criminal investigation does not mean the agents did not mislead him in a way that violates his rights.

Pursuant to *Serlin*, awareness of the “true nature of [the] investigation” is a critical factor. 707 F.2d at 956 (7th Cir. 1983). And this factor is not present simply because the defendant may know in a generic sense that he or she is under a criminal investigation. Instead, knowing the “true nature” involves a greater degree of awareness. As the Seventh Circuit explained:

[s]imple failure to inform defendant that he was the subject of the investigation, or that the investigation was criminal in nature, does not amount to affirmative deceit unless defendant inquired about the nature of the investigation and the agents' failure to respond was intended to mislead.

Id. (emphasis added). And that is exactly what happened here. As noted on pages 19-24 of the Objections, and in earlier defense filings, Mr. Hutchins (repeatedly) inquired about the nature of his arrest and interrogation, and the agents’ (tactical) failure to respond, among other things, was intended to deprive him of important information, details relevant to a person’s decision whether or not to answer questions.

That the agents intentionally confused Mr. Hutchins' about the nature of the investigation, despite his direct inquiries, was revealed prominently when Agent Chartier stated this over an hour into the interrogation:

Okay. Well here's the arrest warrant. And just to be honest—if I'm being honest with you, Marcus. This has absolutely nothing to do with WannaCry.

(Ex. 1 at 1:17:45-1:18:02 (emphasis added).) In sum, Mr. Hutchins' statements can and should be suppressed as a result of the agents' intentional deceit.

F. The Defense Does Not Contend that Foreign Citizens are Immune from U.S. Laws

The government's last section heading is "Foreign citizens like [Mr.] Hutchins are not immune from U.S. laws." This naturally would cause one to think the defense argued as much. It has not.

The defense argument is simply this: Mr. Hutchins' foreign citizenship and what the agents knew about it should be considered in conjunction with the evidence of impairment and, most importantly, deception. The government's opposition fails to properly do this, and as was pointed out in the Objections, the magistrate judge did too.

The government's argument is problematic for other reasons, as well. Notably, it claims "there was no evidence that [Mr.] Hutchins' nationality was exploited in any way." Wrong.

As became crystal clear from the agents' testimony, Mr. Hutchins' arrest at the airport as he was about to fly home to the United Kingdom was designed by the agents to exploit that fact. (*See* Dkt. Not 85 at 5-6.) Before Mr. Hutchins ordered what the agents worried was an alcoholic beverage, they intended to delay his arrest to the last possible moment, as he was about to board his flight home (even though they could have arrested him when he arrived in Las Vegas more than a week before or at any time while he was there). (Tr. 65:8-13 (Chartier); 115:20-116:4 (Butcher).) And even then, two uniformed customs agents arrested him along with Agent Chartier, who was dressed casually and not wearing anything identifying him as an FBI agent. (Tr. 17:12-13 (Chartier).) Thus, there is, in fact, significant evidence that the agents planned to and did exploit the fact that Mr. Hutchins was a foreigner preparing to return home. The Court should consider this.

The government is wrong in the conclusion that the totality of the circumstances do not support suppression. For all the reasons discussed above, in the Objections, and in the record, Mr. Hutchins' interrogation statements should be suppressed, as well as any evidence that may have been gathered as a result of them.

THE MOTION TO DISMISS
(FAILURE TO STATE OFFENSES AND MULTIPLICITY)

Mr. Hutchins seeks dismissal of Counts One through Eight and Ten of the superseding indictment for failure to state offenses on a number of grounds. (Dkt. Nos. 92 & 95.) The Court should decline to adopt the magistrate judge's recommendations that those motions be denied and instead dismiss these counts.

A. "Damage" Under the Computer Fraud and Abuse Act

Defending the sufficiency of Counts One and Seven, the government argues that it needs only to repeat verbatim the language of the invoked statutes to satisfy the pleading requirements of a federal criminal case. (Opp. at 24.) But as discussed in the Objections, the government muddles the distinction between what is technically required as a matter of form and what is substantively necessary. Because the government's characterization of the undisputed facts does not "constitute a violation of any statute," there is "no case to prove."

United States v. Risk, 843 F.2d 1059, 1060 (7th Cir. 1988).

Next, the government attempts to distinguish *Landmark Credit Union v. Doberstein*, 746 F. Supp. 2d 990, 993-94 (E.D. Wis. 2010), and *Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.*, 810 F.3d 1075, 1084 (7th Cir. 2016), by noting that they are civil cases that do not address "criminal pleading standards." (Opp. at 25-26.) But Mr. Hutchins does not cite these cases to establish "criminal pleading standards." He cites them to show that the government has not

pledged a case that alleges “damage” as statutorily defined by the Computer Fraud and Abuse Act (the “CFAA”).

The CFAA’s statutory definitions are the same regardless of whether a case is civil or criminal. So a civil CFAA case interpreting the meaning of “damage” speaks to the meaning of “damage” in a criminal CFAA case, as well. And as this Court pointed out in *Landmark*, the meaning of “damage” for purposes of the CFAA is “very specific.” 746 F. Supp.2d at 993.

Finally, the government leans heavily on the fact that it labeled Kronos and UPAS Kit “malware” in the first superseding indictment, thereby inventing its own definition of that word to mean “malicious computer code intended to damage a computer . . . [that] deletes, creates, and modifies files on a computer[.]” (First Superseding Indictment (“FSI”) ¶ 1(d) (Dkt. No. 86).)

Of course, it is up to Congress rather than employees of the Executive Branch to say what exactly violates the CFAA. And the CFAA does not say “malware” as the prosecution would define it is illegal. Rather, 18 U.S.C. § 1030(a)(5)(A) makes it illegal to “knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer.” And “damage” is specifically defined as “any impairment to the availability or integrity of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8).

In this case, the indictment alleges that Kronos “recorded and exfiltrated user credentials and personal identifying information from protected computers,” (FSI ¶ 1(e)), and that UPAS Kit “allowed for the unauthorized exfiltration of information from protected computers” (*id.* ¶ 1(f)). The superseding indictment does not claim that the programs cause “impairment to the availability or integrity” of the data. Thus, “damage” requires more than what the indictment alleges. Simply copying and taking data in a manner that does not cause disruption or impairment does not meet the statutory definition.

B. “Device” Under the Wiretap Act

The government next defends the magistrate judge’s recommendation that this Court find that Kronos and UPAS Kit are “electronic, mechanical, or other devices” for purposes of 18 U.S.C. §§ 2511 and 2512. (Opp. at 27.) In doing so, the government first points to several cases that did not categorically find, as the government would have it, that “software known as ‘spyware’ or that has keylogger or form grabber functionality falls under the Wiretap Act.” (*Id.*)

To be clear, each of the cases cited by the government considered whether certain *software installed on computers* “intercepted” communications within the meaning of the Wiretap Act. (*Id.* at 27-28, citing *Luis v. Zeng*, 2013 WL 811816, at **3-7 (S.D. Ohio March 5, 2013), *recommendation adopted, reversed on other grounds* by 833 F.3d 619 (6th Cir. 2016); *Carrier IQ, Inc., Consumer Privacy Litig.*, 78 F.

Supp.3d 1051, 1084-87 (N.D. Cal. Jan. 21, 2015); *Shefts v. Petrakis*, No. 10-cv-1104, 2012 WL 4049484, at *9 (C.D. Ill. Sept. 13, 2012); *Klumb v. Goan*, 884 F. Supp.2d 644, 661 (E.D. Tenn. July 19, 2012).) But because none of the defendants in those cases raised the issue (as Mr. Hutchins has), none of the cases expressly considered the critical question of whether the software or the computer was the relevant “device” for purposes of the Wiretap Act.

That makes sense: those cases all involved claims that the defendants acquired communications using software running on a computer. Under those circumstances, the involved courts had no reason to draw a distinction between the software and the computer because the two work in tandem: the operation of one depends on the other. Indeed, every case cited by the government discusses computers and the software installed on them as one unit. *See, e.g., Luis*, 833 F.3d at 633 (“[O]nce installed on a computer, WebWatcher automatically acquires and transmits communications to servers”); *Carrier IQ*, 78 F. Supp.3d at 1059 (“Plaintiffs allege that . . . the Device Manufacturers Defendants embedded[] the Carrier IQ Software on their mobile devices and, once embedded, this software surreptitiously intercepted personal data and communications[.]”); *Klumb*, 884 F. Supp.2d at 661 (“The point is that a program has been installed on the computer which will cause emails sent at some time in the future through the internet to be re-routed[.]”); *see also Shefts*, 2012 WL 4049484, **6-10 (variously referring to

servers, email accounts, software, and BlackBerry smartphones as interception devices).

These cases are all fundamentally different than what the first superseding indictment charges – especially in Counts Two through Five, where Mr. Hutchins is charged with violating 18 U.S.C. § 2512 by allegedly disseminating, sending, and selling the Kronos and UPAS Kit software or aiding and abetting such conduct. For these counts, the distinction between software and computer is important because *there is no computer*, which was not the situation in any case cited by the government. As *Potter v. Havlicek* noted, software by itself – without a computer – is incapable of intercepting anything: “It must be installed in a device, such as a computer, to be able to do so.” 2008 WL 2556723, at *8 (S.D. Ohio June 23, 2008).

The government attempts to distinguish *Potter* – the case that most directly examines the issue of whether software alone can be a wiretapping device – by saying that it deals with manufacturer liability for civil damages under § 2520, which creates a private right of action. (Opp. at 32.) So the government argues that since this is a criminal case, that aspect of *Potter* is irrelevant.

What *is* relevant to this criminal case is *Potter’s* conclusion that the software in that case was not an “electronic, mechanical, or other device” as defined by the Wiretap Act. 2008 WL 2556723, at **8-9. The government neglects

to address this head on, instead pointing to “more recent” cases: *Barrington*, *Carrier IQ*, *Luis*, *Shefts*, and *Klumb*. (Opp. at 32.) As discussed above, all those cases are inapposite because they do not consider whether software in isolation is a wiretapping device, as *Potter* does.

The government also points to *United States v. Barrington* to support its position that keylogger software is an “electronic, mechanical, or other device” under the Wiretap Act. (Opp. at 28, citing 648 F.3d 1178, 1201 (11th 2011).) *Barrington*, however, says no such thing.

That case considered whether a keylogger was “device-making equipment” or a “scanning receiver” under 18 U.S.C. § 1029, which prohibits fraud and related activity in connection with access devices. *Id.* at 1201-02. That statute is not at issue in this case. In fact, the court in *Barrington* concluded there was *no* evidence that the keylogger software at issue was “a device or apparatus that can be used to intercept a wire or electronic communication in violation of [the Wiretap Act].” *Id.* at 1203. If anything, *Barrington* supports Mr. Hutchins’ position, not the government’s.

The government contends that *United States v. Szymuszkiewicz* “did not address the question of whether software qualifies as a device.” (Opp. at 33, citing 622 F.3d 701, 707 (7th Cir. 2010) (as amended Nov. 29, 2010).) But the court there determined that the defendant acquired the relevant communications using

computers. *Id.* The computers were the relevant devices for purposes of the offense. *Id.* Software in isolation was not. So this case supports Mr. Hutchins' position.

Next, the government urges this Court not to adopt the dictionary definition of "device" that the court in *Potter* found to be the most germane for interpreting the Wiretap Act in the absence of a statutory definition of that term. (Opp. at 29.) *Potter* determined that broader dictionary definitions (like those offered by the government) were the wrong fit. 2008 WL 2556723, at *8. Nonetheless, the government offers an array of dictionary definitions to argue that the common meanings of "device," "mechanism," and "apparatus" are far more expansive than the dictionary definition of "device" the *Potter* court found compelling. (Opp. at 29-30.) Yet none of the government's proposed definitions say anything about software, nor provide reason to conclude that software in isolation is an "electronic, mechanical, or other device."

The government contends that Congress drafted "electronic, mechanical, or other device" broadly "in order to accommodate changing technologies." (Opp. at 30-31.) But, in fact, Congress has been careful over time to *limit* the reach of the Wiretap Act, particularly in §§ 2511 and 2512. Notably, Congress chose to increase the level of *mens rea* in §§ 2511 and 2512 from "willful" to "intentional." Electronic Communications Privacy Act, Pub. L. 99-508, Title I, § 101(f), 100 Stat. 1853 (1986).

And even though Congress has amended the Wiretap Act several times since its initial passage in 1968—most recently this year—it has never expanded the definition of “electronic, mechanical, or other device” to include software.⁴ When Congress wishes to make something illegal, it knows how to do so—and it has not done so in the way the government claims. Mr. Hutchins simply urges the Court to construe the Wiretap Act as it has been written.

Finally, in a footnote, the government argues that “Counts One, Two, Three, and Six allege violations of the Wiretap Act that are not dependent on [Mr.] Hutchins’ limited definition of a device.” (Opp. 33-34 n.9.) That is incorrect.

The government first argues that Counts Two and Three should survive because Mr. Hutchins and Individual A allegedly linked to a YouTube video to demonstrate Kronos operating on a computer. (*Id.* at 34 n.9.) But it is not alleged that Mr. Hutchins or Individual A actually made that video or performed any interception shown in it. Thus, according to the government, it is a crime to link

⁴ Pub. L. 90-351, Title III, § 802, 82 Stat. 213 (June 19, 1968); amended Pub. L. 91-358, Title II, § 211(a), 84 Stat. 654 (July 29, 1970); Pub. L. 95-511, Title II, § 201(a) to (c), 92 Stat. 1796, 1797 (Oct. 25, 1978); Pub. L. 98-549, § 6(b)(2), 98 Stat. 2804 (Oct. 30, 1984); Pub. L. 99-508, Title I, §§ 101(b), (c)(1), (5), (6), (d), (f), 102, 100 Stat. 1849 to 1853 (Oct. 21, 1986); Pub. L. 103-322, Title XXXII, § 320901, Title XXXIII, § 330016(1)(G), 108 Stat. 2123, 2147 (Sept. 13, 1994); Pub. L. 103-414, Title II, §§ 202(b), 204, 205, 108 Stat. 4290, 4291 (Oct. 25, 1994); Pub. L. 104-294, Title VI, § 604(b)(42), 110 Stat. 3509 (Oct. 11, 1996); Pub. L. 107-56, Title II, §§ 204, 217(2), 115 Stat. 281, 291 (Oct. 26, 2001); Pub. L. 107-296, Title II, § 225(h)(2), (j)(1), 116 Stat. 2158 (Nov. 25, 2002); Pub. L. 110-261, Title I, §§ 101(c)(1), 102(c)(1), 122 Stat. 2459 (July 10, 2008); Pub. L. 115-141, Div. V, § 104(1)(A), 132 Stat. 1216 (Mar. 23, 2018).

to a video someone else made that shows how malware functions on a computer. This, alone, is not disseminating an advertisement—it is simply displaying how a software program works.

Section 2512(1)(c) does not make it illegal to show or describe how a device (much less software) functions; it makes it illegal to advertise the sale of certain specific prohibited devices. And since § 2512(c)(1) is a restriction on speech, interpreting that section broadly to encompass any communication that demonstrates or describes how a device or software functions would present substantial First Amendment, vagueness, and overbreadth issues. The canon of constitutional avoidance counsels against an expansive construction of this statute. As the Supreme Court has explained, “[W]hen deciding which of two plausible statutory constructions to adopt, a court must consider the necessary consequences of its choice. If one of them would raise a multitude of constitutional problems, the other should prevail—whether or not those constitutional problems pertain to the particular litigant before the Court.”

Clark v. Martinez, 543 U.S. 371, 380-81 (2005).

Turning to Counts One and Six, the government argues that even if Kronos and UPAS Kit do not qualify as “electronic, mechanical, or other devices,” Mr. Hutchins transmitted and conspired to transmit the programs to others knowing and intending for the software to be used to intercept communications in

violation of § 2511(1)(a) and (2). (Opp. at 34 n.9.) The government may be referring to the fact that § 2511(1)(a) prohibits “intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication,” and that section does not specifically mention the use of an “electronic, mechanical, or other device” to do so.

At first blush, § 2511(1)(a) might not appear to require such a device. But the Wiretap Act defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication *through the use of any electronic, mechanical, or other device.*” 18 U.S.C. § 2510(4) (emphasis added). In other words, it is impossible to “intercept” a communication within the meaning of § 2511(1)(a) without using an “electronic, mechanical, or other device” to do so. And because Kronos and UPAS Kit, themselves, are not such devices within the meaning of the Wiretap Act, they cannot as a matter of law intercept communications in violation of § 2511.

The government may instead be attempting to argue that Mr. Hutchins transmitted and conspired to transmit Kronos and UPAS Kit to others who could install the programs on computers, which could then intercept communications in violation of § 2511. Even assuming that others installed Kronos and UPAS Kit on computers that would qualify as devices, the allegations in Counts One and

Six do not support the conclusion that Mr. Hutchins conspired to transmit or transmitted the programs to others knowing and intending for those people to intercept communications. The superseding indictment does not allege that Mr. Hutchins intended a buyer to do anything in particular, as discussed in more detail in the next section.

C. Intent and Causation

Mr. Hutchins asks the Court to dismiss Counts One, Four through Eight, and Ten for their failure to allege the necessary intent and causation to state the offenses. (Obj. at 35-37.) The government argues that the recommended denial of this motion is proper because Mr. Hutchins' challenge is to the sufficiency of the evidence, rather than the allegations of the superseding indictment. (Opp. at 34-35.)

The government misapprehends Mr. Hutchins' argument. Mr. Hutchins does not challenge the sufficiency of the evidence at this stage in the case. Rather, these counts, as alleged, are missing the specific intent necessary to allege criminal conduct. Thus, the Court should dismiss Counts One, Four through Eight, and Ten.

D. Motion to Dismiss Counts Two and Three as Multiplicitous

Mr. Hutchins argues that Counts Two and Three are multiplicitous, exposing Mr. Hutchins to double jeopardy. (Obj. at 37-38.) The government

argues that this motion should be denied because “Count Three contains an additional element” that Count Two does not. (Opp. at 36.)

But Counts Two and Three do not *each* require proof of an additional fact that the other does not. Each count requires proof of the same facts, as explained in the underlying motion. (Dkt. No. 95 at 11.) Specifically, § 2512(1)(c)(i) prohibits the advertisement of an interception device when one *knows or has reason to know that the design of the device renders it primarily useful for the purpose of surreptitious interception*. And § 2512(1)(c)(ii) prohibits the advertisement of an interception device in a manner that *promotes its use for the purpose of surreptitious interception*. The same fact proves the offense charged in Count Two and Count Three: when one advertises a device designed for surreptitious interception, he promotes its use for surreptitious interception.

When an indictment is multiplicitous, “it may prejudice the jury against the defendant by creating the impression of more criminal activity on his part than in fact may have been present.” *United States v. Marquardt*, 786 F.2d 771, 778 (7th Cir. 1986) (quoting *United States v. Carter*, 576 F.2d 1061, 1064 (3rd Cir. 1978)). To avoid such prejudice, the Court should reject the government’s suggestion that merger solves the cited multiplicity. (Opp. at 14-15.) If the Court does not dismiss Count Three outright, it should at a minimum exercise its discretion to order the government to elect to proceed with either Count Two or Count Three.

See United States v. Johnson, 130 F.3d 1420, 1426 (10th Cir. 1997) (election avoids the possibility of falsely suggesting more criminal behavior to the jury than in fact occurred).

THE MOTION TO DISMISS
(COUNT SEVEN)

Objecting to the recommendation that his motion to dismiss Count Seven be denied, Mr. Hutchins explains that the recommendation interprets the indictment and § 1030(a)(5)(A) in a way establishing a crime different from any Congress has defined and contrary to traditional understandings of inchoate offenses. (Obj. at 38-40.)

The government's response makes no attempt at explaining how it is permissible to charge an attempted violation of § 1030(a)(5)(A) in a way that treats only part of the offense—the intended outcome—as attempted. Instead, the government argues only that accepting Mr. Hutchins' argument “would eviscerate liability for . . . attempts to violate § 1030.” (Opp. at 38.) That is incorrect.

As stated in the Objections, attempting a crime involves intending to complete the full crime, as Congress defines it in elemental fashion, then taking a substantial step towards that crime's commission. (Obj. at 39-40.) Applying those established principles to attempted violations of § 1030(a)(5)(A) does not, as the government contends, produce a situation in which an attempted violation

of the statute can't be established short of a completed crime. (*Id.* at 38.) Instead, the Seventh Circuit's approach to attempts requires that an attempted violation of § 1030(a)(5)(A) be charged as "the defendant attempted to transmit a program and, as a result, intentionally cause damage to a protected computer." *See* 18 U.S.C. § 1030(a)(5)(A).

Only by this approach does an indictment charging an attempted violation of § 1030(a)(5)(A) satisfy the general requirement that the intent accompanying an inchoate crime reach each of the substantive crime's elements, including that crime's required mental state. *United States v. Morris*, 827 F.3d 696, 699 (7th Cir. 2016) (Hamilton, J., concurring) (explaining that "an attempt to commit a crime should be treated as an attempt to carry out acts that satisfy *each element of the completed crime*"') (emphasis in original)).

Count Seven of the indictment fails to honor those principles and the recommendation that Mr. Hutchins' motion to dismiss the court be denied should not be adopted.

THE MOTION TO DISMISS
(IMPROPER EXTRATERRITORIAL APPLICATION OF LAW)

The government advances two main arguments in response to Mr. Hutchins' motion to dismiss due to improper extraterritorial application of U.S. law. First, the government contends that Counts Two and Three are a domestic application of the Wiretap Act, 18 U.S.C. § 2512(1)(c), and in any event, that law

should have extraterritorial application. (Opp. at 39-46.) Second, the government asserts that Mr. Hutchins needs no sufficient nexus with the U.S. to be prosecuted here for his conduct abroad. (Opp. at 46-48.)

These arguments miss the mark for two reasons. First, the superseding indictment does not plead a domestic application of § 2512(1)(c) in Counts Two and Three. Second, the sufficient nexus requirement rooted in the Fifth Amendment due process clause applies in all cases—including this one. Finally, Count Nine should be dismissed because Mr. Hutchins cannot be guilty of making a false statement in a matter within U.S. government jurisdiction if the rest of this case is dismissed for the reasons in the defense motion.

A. Counts Two and Three Constitute an Unlawful Extraterritorial Application of the Wiretap Act, Not Domestic

The magistrate judge's order and recommendations found that Counts Two and Three plead a domestic application of § 2512(1)(c). (Rec. at 30-31.) As such, the magistrate judge found it unnecessary to determine whether the Wiretap Act has extraterritorial application. (*Id.* at 32.) Nonetheless, the government continues to argue that Counts Two and Three are domestic applications of § 2512(1)(c), and that the Wiretap Act has extraterritorial application regardless. (Opp. at 39-46.) This is misplaced.

1. The First Superseding Indictment Does Not Allege Domestic Application of the Wiretap Act in Counts Two and Three

The government argues that the Wiretap Act charges in Counts Two and Three are domestic in nature because the conduct alleged in those counts purportedly occurred in the U.S. (Opp. at 39.) This argument is based on just two allegations: (1) that Mr. Hutchins and Individual A used a YouTube video to advertise and promote Kronos; and (2) that the YouTube video and other advertisements on other internet forums were viewed in this District, and an individual in this District was specifically directed to the YouTube video. (*Id.*) These bare claims do not properly plead a domestic application of § 2512(1)(c).

Taking the government's two arguments in turn, we first consider the YouTube video. The superseding indictment alleges that a video showing the functionality of Kronos was "posted to YouTube." (FSI ¶ 4(e).) It is not alleged, however, that Mr. Hutchins or Individual A posted the video themselves. Rather, Mr. Hutchins and Individual A allegedly "used the video to demonstrate how Kronos worked and to promote the sale of Kronos." (*Id.*) So this government argument fails.

In an attempt to resurrect it, the government notes that YouTube is a U.S.-based platform. (Opp. at 39.) Yet the government offers no authority for the proposition that the mere fact a corporation maintains its headquarters in the U.S. subjects any conduct tangentially involving the corporation to a domestic

application of federal criminal law. No essential conduct element occurred in the U.S. just because YouTube’s main office happens to be located here. Neither Mr. Hutchins nor Individual A is purported to have posted the video or otherwise had any direct connection to YouTube. Nor is it claimed that the video was hosted on a server in the U.S. Indeed, Google, which owns YouTube, hosts data on servers located throughout the world.⁵

Under the government’s apparent theory, then, a foreign citizen who sends another person a link to a video can subject himself to prosecution under § 2512 – even when the sender did not post the video, and even when the video is hosted on a server in another country – so long as the company that owns the server happens to be headquartered somewhere in the U.S.⁶ The Court should reject the government’s theory.

Next, the government contends that Individual A’s posts and the YouTube video “were viewed in the Eastern District of Wisconsin, and in the case of the

⁵ Google Data Centers, <https://www.google.com/about/datacenters/inside/locations/index.html> (last visited December 7, 2018). Even assuming for the sake of argument that the video’s posting on YouTube creates some domestic link in this case, it does not create any nexus to this District. YouTube is headquartered in San Bruno, California. The government offers no explanation why the prosecution of Mr. Hutchins in Wisconsin is proper due to a company based in another state.

⁶ If other countries were to apply the government’s proposed rule to U.S. citizens, nations such as Russia and China might choose to prosecute people living in this country for linking to material on the Internet that those governments consider objectionable – but is perfectly lawful here – under the rationale that U.S. citizens have violated the law within those nations. That result would untenable.

YouTube video, an individual in the Eastern District of Wisconsin was specifically directed to it and viewed in this district.” (Opp. at 39.) But the superseding indictment does not plead this version of events. It does not allege that Mr. Hutchins or Individual A directed the video to an individual in this District, used the video to demonstrate anything to an individual in this District, or that the video was viewed by anyone in this District. It includes only a vague statement that Counts Two and Three generally occurred “in the state and Eastern District of Wisconsin and elsewhere.”

As in its first round of motions to dismiss, the government asks the Court to look outside the four corners of the superseding indictment to salvage these counts. But Federal Rule of Criminal Procedure 12(d) does not permit this.

United States v. Bryant, 2013 WL 3423275, at **5-6 (E.D. Wis. July 8, 2013).

More importantly, while the government characterizes the viewing of the purported advertisements as domestic “acts” that subject Mr. Hutchins to prosecution in this country (Opp. at 39), these are not the “acts” of Mr. Hutchins or Individual A, nor are they the “acts” that § 2512(1)(c) is intended to punish. The statute prohibits the intentional dissemination of advertisements and promotion of a certain category of device. Thus, the relevant conduct is the publication of prohibited advertisements and promotions.

But there is no allegation that Mr. Hutchins or Individual A undertook any such publication from within the U.S., or that either Mr. Hutchins or Individual A intentionally directed any advertisement or promotion toward someone they knew to be inside the U.S. The government does not even allege that Mr. Hutchins intended Individual A to market or promote Kronos in the U.S.

The superseding indictment alleges only that the co-conspirators advertised Kronos to the world at large. And the government claims now – and outside the four corners of the first superseding indictment – that someone within this District received and viewed advertisements posted on non-U.S. internet forums, as well as the YouTube video. This argument must be rejected.

An offense cannot be prosecuted anywhere in the world just because it involves the Internet. The World Wide Web does not grant the Department of Justice worldwide authority. To the extent that the government believes Mr. Hutchins may be prosecuted in this District, he could be prosecuted anywhere in the world, under the laws of any country – and there is no reason other countries could not prosecute our citizens the same way. That is the wrong result.

2. The Wiretap Act Does Not Have Extraterritorial Application

The government next argues that § 2512 is a criminal statute whose language and function is intended to protect a U.S. interest, so it applies extraterritorially as a matter of course. (Opp. at 41.) The government insinuates

that the magistrate judge’s order and recommendations agreed with this assessment, when, in fact, it determined that it was “unnecessary to address whether the Wiretap Act applies extraterritorially.” (Rec. at 32.) In any event, the government’s position is inconsistent with the precedent of the Supreme Court and Seventh Circuit.

First, the government argues that the Wiretap Act falls within a class of criminal statutes that should have extraterritorial application by their very nature. (Opp. at 41.) As such, according to the government, § 2512 should reach foreign citizens acting outside the U.S., even if Congress has not actually expressed any intent for the law to extend abroad.

The foundation of this argument is *United States v. Bowman*, 260 U.S. 94 (1922), the holding of which is nowhere remotely as broad as the government suggests. In *Bowman*, four people—three U.S. citizens and a British citizen—were charged with conspiring to defraud a shipping company wholly owned by the U.S. government. *Id.* at 95. The defendants committed the offense on the high seas, outside the jurisdiction of any state or district, “but within the admiralty and maritime jurisdiction of the [U.S.]” *Id.* at 96. The Supreme Court thus faced the question of where a crime occurs when Congress has not specifically identified its locus.

The Supreme Court began by observing that a wide range of crimes “against private individuals or their property . . . and frauds of all kinds” do not have extraterritorial effect unless Congress explicitly says otherwise. *Id.* at 98. It then carved out a narrow category of criminal statutes “which are, as a class, not logically dependent on their locality for the government’s jurisdiction, but are enacted because of the *right of the government to defend itself* against obstruction, or fraud wherever perpetrated, *especially if committed by its own citizens, officers, or agents.*” *Id.* (emphasis added).⁷ As the Court went on to explain, limiting such crimes to the territorial jurisdiction of the U.S. “would be greatly to curtail the scope and usefulness of the statute and leave open a large immunity for frauds as easily committed *by citizens* on the high seas and in foreign countries as at home.” *Id.* at 98 (emphasis added).⁸

Importantly, the *Bowman* holding was about U.S. citizens who were working for—and directly conspired against—a corporation wholly owned by the U.S. *Id.* at 94–95. In addition to the three U.S. citizen defendants to whom the Court’s holdings applied, the fourth defendant, a “subject of Great Britain,” had not been apprehended. *Id.* at 102. The Court specifically declined to address

⁷ The government quotes this language on page 42 of its response, doing so without the important phrase “especially if committed by its own citizens, officers, or agents.”

⁸ Again, the government quotes this language on page 42 of its response, but omits the words “by citizens.” This omission might be read to create an erroneous impression that the Supreme Court extended its reasoning to apply to non-citizens, as well, which it did not.

the application of U.S. law to that defendant, concluding that there “will be time enough to consider what, *if any*, jurisdiction the District Court below has to punish him when he is brought to trial.” *Id.* at 102–03 (emphasis added).

So *Bowman* does not broadly authorize the imposition of federal criminal law abroad to foreign citizens and residents whose alleged actions were committed outside of the U.S. It defines a narrow class of statutes that are “enacted because of the government’s right to defend itself,” especially against offenses committed by “its own citizens, officers, or agents,” and permits extraterritorial application in that limited circumstance. *Id.* at 98.

The Wiretap Act does not fall within that category. Congress enacted this law to protect the privacy of people’s communications. S. Rep. No. 90-1097, 90th Cong., 2nd Sess. (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2156. Section 2512(1)(c) in particular was enacted to “curtail the supply” of devices designed primarily for the purpose of eavesdropping on people’s private communications. *Id.* at 2183. Thus, the Wiretap Act is a crime “against private individuals” for which Congress must explicitly authorize extraterritorial application under *Bowman*. 260 U.S. at 98. The fact that a government agent may have viewed an alleged advertisement or promotion does not change Congress’ original purpose for enacting the law.

Nor did the Seventh Circuit broadly authorize extraterritorial application of criminal law in *United States v. Leija-Sanchez*, 602 F.3d 797, 798-99 (7th Cir. 2010) (*Leija-Sanchez I*), and *United States v. Leija-Sanchez*, 820 F.3d 899, 900-01 (7th Cir. 2016) (*Leija-Sanchez II*). The magistrate judge's order and recommendations discusses *Leija-Sanchez I* and the government relies heavily on these decisions (see Rec. at 31 & Gov't Response at 41-45). However, that case is not factually analogous to this case.

In *Leija-Sanchez*, the defendant was prosecuted for a variety of crimes stemming from the activities of a criminal organization that produced fraudulent identification documents. Among other offenses, the defendant was charged under the RICO statute (§ 1959) for arranging and paying for the murder of a competitor. The murder was organized and paid for from the U.S., but it was carried out in Mexico. The district court dismissed the § 1959 charge, concluding that the statute did not reach the murder abroad. The government appealed, arguing that § 1959 has extraterritorial application.

In *Leija-Sanchez I*, the Seventh Circuit considered whether the murder's occurrence abroad precluded the defendant's prosecution under § 1959 in the U.S. Applying *Bowman*, the court noted that the case "does not hold that criminal statutes always apply extraterritorially," but rather "judges must consider the language and function of the prohibition." *Id.* at 799. The district

court looked to the text of § 1959, which states that the law applies to organizations engaged in “foreign commerce.” *Id.* at 799-800. But it ultimately found that all of the conduct ascribed to the defendant—the planning and payment—took place in the U.S. and had significant consequences in this country. *Id.* at 800-01. So despite the murder abroad, the case had sufficient connections to the U.S. to prosecute the defendant here. In effect, the court authorized a domestic application of § 1959, not an extraterritorial one.

Later, the Seventh Circuit revisited the case after the defendant’s conviction and the Supreme Court’s extraterritoriality decision in *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247, 261 (2010). *Leija-Sanchez II*, 820 F.3d 899. The Seventh Circuit stood by its analysis in *Leija-Sanchez I* for two reasons. First, it believed that *Bowman*, rather than *Morrison*, should apply in the criminal context, *id.* at 901—but did not address *Morrison*’s clear directive that the presumption against extraterritoriality applies in “all cases.” *Morrison*, 561 U.S. at 261. Second, the Seventh Circuit reiterated that the murder was organized in and had “ample links” to the U.S. 820 F.3d at 901.

Leija-Sanchez I & II did not involve a situation like this case, in which the government is prosecuting a foreign national residing in another country whose

actions were performed abroad.⁹ It is not clear what the Seventh Circuit would have found in such a case, and *Leija-Sanchez I & II* do not shed much light on that question because they involve a different statute and rely heavily on the defendant's acts within the U.S.

Furthermore, when deciding *Leija-Sanchez I & II*, the Seventh Circuit did not yet have the benefit of the Supreme Court's most recent extraterritoriality decision in *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090, 2100 (2016). *RJR Nabisco* directly addressed the extraterritorial application of the RICO statute (which, like the Wiretap Act, has both criminal and civil applications). See 136 S. Ct. at 2101-2103.

The Supreme Court held that RICO can apply extraterritorially – but *only* to the extent that the predicate offenses *themselves* apply extraterritorially. *Id.* at 2101. The Court “emphasize[d] the important limitation that foreign conduct must violate a predicate statute that manifests an unmistakable congressional intent to apply extraterritorially.” *Id.* at 2102 (internal quotation marks omitted).

And importantly, the Supreme Court “emphatically rejected” the notion that the phrase “foreign commerce” in a statute is sufficient to show that

⁹ The magistrate judge's order and recommendations contend that the defense fails to take into account that the indictment “alleges conduct ‘occurring in the state of Wisconsin and elsewhere.’” (Rec. at 31.) As discussed in the section above, the superseding indictment's bare claims are insufficient to allege a domestic application of § 2512(1)(c), much less substantial enough to justify an extraterritorial application of the law over Mr. Hutchins.

Congress intended that law to apply abroad. *RJR Nabisco*, 136 S. Ct. at 2110. To the extent that *Leija-Sanchez I & II* suggest otherwise, they are inconsistent with the Supreme Court's extraterritoriality precedent.

While *RJR Nabisco* was a civil case, the Supreme Court did *not* suggest that the presumption against extraterritoriality would apply differently depending on whether a RICO case is criminal or civil. Indeed, *Bowman* suggests that a statute that is both criminal and civil should be interpreted consistently in both contexts. 260 U.S. at 98 ("That was a civil case, but as the statute is criminal as well as civil, it appears an analogy."). That makes sense and is consistent with the rule of lenity, which suggests that statutes with both criminal and civil applications should not be interpreted in a manner that treats criminal defendants more harshly than civil defendants. See *Skilling v. United States*, 561 U.S. 358, 365 (2010) ("ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity," and broad constructions "should be rejected absent Congress' clear instruction otherwise.").

The government applies "the extraterritoriality analysis from *Bowman* and *Leija-Sanchez I*" to conclude that § 2512 should apply abroad. (Opp. at 44.) Under this analysis, according to the government, "a court first considers the 'language and function' of the statute to determine if the 'conduct proscribed

causes or is likely [to] cause significant injury to the U.S.’’ (*Id.*, attributing quote to *Leija-Sanchez I*.) This proposed test has two serious flaws.

First, neither *Bowman* nor *Leija-Sanchez I* requires a court to determine if the “conduct proscribed causes or is likely [to] cause significant injury to the U.S.” This language does not appear in either case (despite the fact that it is presented as a direct quote from *Leija-Sanchez I*).

Second, *Leija-Sanchez I* attributes the “language and function” standard to *Bowman* without citation. But this language does not appear in *Bowman*. 602 F.3d at 799.

Under the Supreme Court’s recent line of extraterritoriality cases, a two-step test determines whether a statute has extraterritorial application. A court first asks whether “the statute gives a clear, affirmative indication that it applies extraterritorially.” *RJR Nabisco*, 136 S. Ct. at 2101. If it does not, a court determines whether the case involves a domestic application of the statute by looking to the “focus” of congressional concern. *Id.* at 2101; *Morrison*, 561 U.S. at 249.

Section 2512(1)(c) does not give a clear, affirmative indication that it is meant to apply extraterritorially. The only language in the provision that could arguably support that conclusion is the use of the phrase “foreign commerce.” But the Supreme Court has repeatedly found that a statute’s use of this generic

phrase, with nothing more, does not satisfy the standard. *RJR Nabisco*, 136 S. Ct. at 2110; *Morrison*, 561 U.S. at 262-63; *EEOC v. Arabian American Oil Co.*, 499 U.S. 244, 248 (1991).

Nor does the legislative history reflect that Congress had any intention to extend the reach of § 2512 abroad. The Senate Report drafted at the time of § 2512's passage made a point to say that "there is no intent to preempt State law" – but it did not express any intent that the statute should have extraterritorial application. S. Rep. 90-1097, at 57 (1968).

Thus, we turn to whether this case involves a domestic application of § 2512 by looking to the "focus" of congressional concern. The superseding indictment does not charge a domestic application of § 2512, as discussed at length above in the section above. Thus, Counts Two and Three are an improper attempt to apply U.S. law to the foreign acts of a foreign citizen.

B. The First Superseding Indictment Does Not Allege a Sufficient Nexus and Violates Mr. Hutchins' Due Process Rights

The government apparently rejects the notion that there is any Fifth Amendment limitation to its prosecution of foreign citizens whose acts occur abroad. This is wrong.

The government notes that no statute charged in this case requires the showing of a sufficient nexus between Mr. Hutchins and the U.S. (Opp. at 47.)

The defense agrees. The sufficient nexus requirement is not a creature of any particular statute, but rather a Fifth Amendment due process right. In *United States v. Perlaza*, for instance, the Ninth Circuit explained:

In addition to the [Maritime Drug Law Enforcement Act]’s statutory jurisdiction requirements, where the MDLEA is being applied extraterritorially, as in this case, due process requires the Government to demonstrate that there exists a sufficient nexus between the conduct condemned and the [U.S.] such that the application of the statute would not be arbitrary or fundamentally unfair to the defendant.

439 F.3d 1149, 1160 (9th Cir. 2006) (internal quotation marks omitted); *see also United States v. Davis*, 905 F.2d 245, 248 (9th Cir. 1990) (“[A]s a matter of constitutional law, we require that application of the statute to the acts in question not violate the due process clause of the Fifth Amendment.”); *United States v. Klimavicius-Viloria*, 144 F.3d 1249, 1257 (9th Cir. 1998) (the sufficient nexus requirement is a “judicial gloss to ensure that a defendant is not improperly haled into court for trial” and “serves the same purpose as the ‘minimum contacts’ test in personal jurisdiction”).

The government cites two cases purportedly rejecting the required showing of a Fifth Amendment sufficient nexus in MDLEA cases. (Opp. at 47, citing *United States v. Cardales*, 168 F.3d 548, 552-53 (1st Cir. 1999) and *United States v. Martinez-Hidalgo*, 993 F.2d 1052, 1056 (3d Cir. 1993).) But those two cases did not conclude that the defendants had no due process rights to safeguard.

They simply found that due process did not require the showing of a nexus under the specific circumstances of those cases.

In *Cardales*, the First Circuit concluded that when foreign nationals engage in drug trafficking on a vessel in waters under U.S. jurisdiction, “*due process is satisfied* when the foreign nation in which the vessel is registered authorizes the application of U.S. law to the persons on board the vessel.” 168 F.3d at 553 (emphasis added). This is because the foreign nation’s agreement “eliminates any concern that the application of U.S. law may be arbitrary or fundamentally unfair.” *Id.*

And in *Martinez-Hidalgo*, the Third Circuit held that the government did not need to establish a sufficient nexus specifically for MDLEA cases because it believed Congress meant for the MDLEA to have extraterritorial application, and because drug trafficking is “condemned universally.” 993 F.2d at 1056. But the Third Circuit did *not* find that a sufficient nexus is never required to apply U.S. law abroad. Indeed, it specifically acknowledged that “there might be a due process problem if Congress provided for the extraterritorial application of U.S. law to conduct on the high seas without regard for a domestic nexus if that conduct were generally lawful throughout the world.” *Id.*

Here, Mr. Hutchins simply asks this Court to recognize, and enforce, his due process right to be tried only in a court into which he could reasonably expect to be haled.

C. Count Nine Should be Dismissed

Count Nine, which charges a violation of 18 U.S.C. § 1001, relates to a purported statement Mr. Hutchins made when the FBI questioned him about his alleged actions abroad at a time when he had an insufficient nexus to the U.S. And the phrase “matter within the jurisdiction,” as used in § 1001, means that the department or agency has “the power to exercise authority in a particular situation.” *United States v. Rogers*, 466 U.S. 475, 479 (1984).

Because the FBI had no “power to exercise authority” against Mr. Hutchins based on his conduct abroad that had no substantial nexus to the U.S., the FBI was questioning him about a matter outside its jurisdiction. Any purportedly false statements of Mr. Hutchins thus should not be able to form the basis of a criminal charge against him if Counts One through Eight and Ten are dismissed.

CONCLUSION

For all the above reasons and those in the underlying defense objections and motions, the Court should grant the motion to suppress and motions to dismiss.

DATED: December 7, 2018

Respectfully submitted,

/s/ Brian E. Klein

BRIAN E. KLEIN
Baker Marquart LLP
2029 Century Park E - Suite 1600
Los Angeles, CA 90067
Email: bklein@bakermarquart.com
Telephone: (424) 652-7800

/s/ Marcia Hofmann

MARCIA HOFMANN
Zeitgeist Law PC
25 Taylor Street
San Francisco, CA 94102
Email: marcia@zeitgeist.law
Telephone: (415) 830-6664

/s/ Daniel W. Stiller

DANIEL W. STILLER
DStillerLLC
Box 511130
Milwaukee, WI 53203
Email: dan@dstillerllc.com
Telephone: (414) 207-3190

Attorneys for Marcus Hutchins